

Attorney Docket No. 06666-032001
Serial No. 09/576,598
Amendment dated June 30, 2004
Reply to Office Action dated March 30, 2004

Amendment to the Claims:

This listing of claims replaces all prior versions, and listings, of claims in the application:

1. (Currently amended) A cryptography method, comprising:
determining information to be encrypted, and
encrypting said information using a non-trivial ci-quasigroup to encode said information ~~an arithmetic which is not associative.~~

2. (Canceled)

3. (Currently amended) A method as in claim [[2]] 1,
further comprising decoding said information using the crossed-inverse function of said ci-quasigroup.

4. (Currently amended) A method as in claim[[s]] 1-~~or~~ 2,
wherein said encrypting comprises carrying out a first encryption to get a first result, then carrying out a second encryption using said first result, and said encryption can be iterated an arbitrary number of times.

Attorney Docket No. 06666-032001
Serial No. 09/576,598
Amendment dated June 30, 2004
Reply to Office Action dated March 30, 2004

5. (Currently amended) A method as in claim [[2]] 1 further comprising defining a rule indicative of said quasigroup.

6. (Original) A method as in claim 3 further comprising defining a rule indicative of said crossed inverse of said quasigroup.

7. (Original) A method as in claim 1 further comprising carrying out a second encrypting using said arithmetic, and wherein a result of said second arithmetic is encrypted exponentially more than a result of said first arithmetic.

8. (Currently amended) A method as in claim 1 wherein said encrypting comprises using a non trivial [[a]] non-group crossed inverse quasigroup to encode.

9. (Original) A method as in claim 3 further comprising distributing information indicative of said quasigroup as a public key, and keeping secret the crossed inverse quasigroup.

Attorney Docket No. 06666-032001
Serial No. 09/576,598
Amendment dated June 30, 2004
Reply to Office Action dated March 30, 2004

10. (Original) A method as in claim 2 wherein said quasigroup is formed by an n by n square, where n is greater than 10^{10} .

11. (Original) A method as in claim 4 wherein said first and second encryption form iterative encipherment.

12. (Original) A method as in claim 4 wherein said first interiation is carried out in a different direction than said first encryption.

13. (Original) A method as in claim 12 wherein said first direction is left to right and said second direction is right to left.

14. (Original) A method as in claim 1 wherein said encrypting is carried out using block ciphers.

15. (Original) A method as in claim 14 wherein said block cipher are defined by a function.

16. (Original) A method as in claim 14 wherein said block ciphers are formed using cross inversed quasigroups, used

Attorney Docket No. 06666-032001
Serial No. 09/576,598
Amendment dated June 30, 2004
Reply to Office Action dated March 30, 2004

according to $C = f(M, K)$ for the encryption and $M = f_{inv}(C, K)$ for the decryption.

17-18. (Canceled)

19. (Currently amended) A cryptography method, comprising:
determining information to be encrypted; and
encrypting said information using ~~an arithmetic which is~~
~~not commutative~~ a crossed-inverse quasigroup.

20. (Canceled)

21. (Original) A method as in claim 19, further comprising
decoding using a crossed inverse of said quasigroup.

22. (Original) A method as in claim 1, wherein said
encrypting comprises carrying out a first encryption to get a
first result, then carrying out a second encryption using said
first result.

23. (Original) A cryptography method comprising encrypting
information using an arithmetic with an algebraic structure,
said algebraic structure being a nongroup, nonfield structure.

Attorney Docket No. 06666-032001
Serial No. 09/576,598
Amendment dated June 30, 2004
Reply to Office Action dated March 30, 2004

24. (Original) A method as in claim 23 wherein said algebraic structure is not associative.

25. (Original) A method as claim 23 wherein said algebraic structure is not commutative.

26. (Original) A method as in claim 24 wherein said algebraic structure is not commutative.

27-28. (Canceled)

29. (Currently amended) An apparatus comprising a program stored on a computer readable media including instructions to:

encrypt a message using a ~~non-associative arithmetic~~
information indicative of a crossed-inverse quasigroup
representation; and

send the encrypted message; and

decrypt the message using information indicative of the
same crossed-inverse quasigroup representation.

30. (Canceled)

Attorney Docket No. 06666-032001
Serial No. 09/576,598
Amendment dated June 30, 2004
Reply to Office Action dated March 30, 2004

31. (Original) An apparatus as in claim 29, wherein said arithmetic is one which is based on a multiplication table which is expressed as a rule.

32. (Original) An apparatus as in claim 29, further comprising adding a random seed to said arithmetic.

33. (Original) An apparatus as in claim 30, further comprising using an additional encryption to provide an effective key size of x^2 of the original encryption.

34. (Canceled)